09/438 342

ABSTRACT

A method and apparatus for efficiently synchronizing a stream cipher. State information is transmitted that will allow the intended recipient of the encrypted data stream to set a stream cipher generator to the correct state from which to start generating the stream cipher. A cycle number indicating the current state of a linear feedback shift register and a stutter number indicating whether an output of the linear feedback shift register is dropped are both transmitted to a remote station along with the encrypted data stream.